UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

R.C., et al.,

Plaintiffs,

v.

SUSSEX PUBLISHERS, LLC,

Defendant.

Case No. 24-cv-02609-JSC

ORDER RE: DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' SECOND AMENDED COMPLAINT

Re: Dkt. No. 42

Plaintiffs R.C. and D.G. (collectively "Plaintiffs") bring this putative class action against Sussex Publishers, LLC claiming it disclosed and mishandled their private and medical information in violation of California law. (Dkt. No. 36.)[1] Defendant now moves to dismiss the Second Amended Complaint ("SAC") on the grounds Plaintiffs lack standing and have not stated a plausible claim. (Dkt. No. 42.) After carefully considering the parties' written submissions, and having had the benefit of oral argument on February 27, 2024, the Court GRANTS in part and DENIES in part Defendant's motion.

BACKGROUND

I. SAC Allegations

Defendant owns the website ww.psychologytoday.com (the "website" or the "site") which "publishes content written by clinicians, experts, and researchers from across the field of behavior and psychology." (Dkt. No. 36 ¶ 27.) The site "facilitates the provision of mental health services by listed therapists" and features "a button and link for consumers to contact therapists directly," "send[s] consumers emails with copies of their private communications to therapists containing

[1] Record citations are to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of the documents.

medical information" and "dates and times of their scheduled appointments," and Defendant "host[s] teletherapy sessions on the Psychology Today website or mobile app." (*Id.* ¶ 28.)

"Google Analytics code is embedded into the Psychology Today website." (*Id.* ¶ 6.) "When a user accesses a website hosting Google Analytics, Google's code surreptitiously directs the user's browser to duplicate the communication with the host website and concurrently send that copied message to Google's servers." (*Id.* ¶ 40.) Google thus collects "a user's interactions in real-time as the user navigates the page." (*Id.* ¶ 41.) "That includes [] any information that the user may input and the links that the user clicked." (*Id.*)

Defendant maintains a "free online directory that lists clinical professionals, psychiatrists, treatment centers, and support groups providing mental health services." (*Id.* ¶ 48.) Users can access the directory either by using a search function or by clicking on the "Find a Therapist" link. (*Id.* ¶ 49.) Using this link, a user inputs their desired "city or zip code" and then clicks various filters to narrow their search, "specifying [their] mental health concerns, insurance provider, gender preference, type of therapy sought, age range treated, price, and many other preferences." (*Id.*) Use "of this feature yields a list of potential therapists." (*Id.* ¶ 51.) The site includes a function whereby a user could "click a telephone number or telephone icon to place a call or, alternatively, they can click an 'Email me' button that pops up a browser window with a fillable form." (*Id.* ¶ 52.) The user can then send an email directly to the provider. (*Id.*)

Because Defendant allows Google Analytics to run on its site, Google is able to, "in real-time, surreptitiously [] duplicat[e] and collect[] users' sensitive information." (*Id.* ¶ 56.) "In addition to IP addresses, that personal information includes but is not limited to (1) the user's specific medical or mental health symptoms and concerns giving rise to the need for therapy; (2) the type of care or treatment that the user is requesting; (3) information concerning the user's gender, ethnicity, and faith preferences regarding the therapist; (4) the city or zip code where the user is seeking therapy sessions; (5) the user's health insurance provider; and (6) information regarding the mental health providers viewed and/or contacted if that was done directly through the website." (*Id.* ¶ 56.)

Google offers an anonymization feature for its Analytics code which automatically

anonymizes the user's IP address, but Defendant "did not enable or utilize Google's IP anonymization feature before the Complaint was filed." (*Id.* ¶¶ 62, 64.)[2] Plaintiff R.C. used the site's filters, "which reflected his symptoms and the type of therapy he was seeking" to find a therapist in his zip code who accepted his insurance. (*Id.* ¶ 12.) He was not aware nor did he consent to this information being simultaneously shared with Google. (*Id.* ¶ 16.) Plaintiff D.G. used the same feature multiple times from November 7, 2019 through 2023, using the filter options for "symptoms and issues indicating her mental health concerns and need for treatment," as well as her faith, her zip code, and her insurer. (*Id.* ¶¶ 19-20.)

II. Procedural Background

Plaintiffs filed the operative SAC on October 31, 2024 alleging the following claims:

(1) California Medical Information Act ("CMIA"),

(2) California Consumer Privacy Act ("CCPA"),

(3) aiding and abetting liability for unlawful interception by Google pursuant to California Penal Code 631,

(4) unlawful eavesdropping under California Penal Code § 632, and

(5) invasion of privacy under Article I § 1 of the California Constitution.

(Dkt. No. 36.) Defendant moves to dismiss Plaintiffs' complaint under Federal Rule of Civil Procedure 12(b)(1) for failure to allege a concrete and particularized injury sufficient to confer standing. (Dkt. No. 42.) Defendant alternatively moves to dismiss the SAC under Rule 12(b)(6) for failure to state a claim upon which relief may be granted. (*Id.*)

ANALYSIS

I. Motion to Dismiss for Lack of Jurisdiction (Rule 12(b)(1))

A jurisdictional attack may be factual or facial. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). A facial attack "asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). "The district court resolves a facial attack as it would a motion to dismiss under

[2] As of the time of the SAC filing, Google's latest iteration of its Analytics code automatically anonymizes all IP addresses. (*Id.* ¶ 8 n.3.)

Rule 12(b)(6): Accepting the plaintiff's allegations as true and drawing all reasonable inferences in the plaintiff's favor, the court determines whether the allegations are sufficient as a legal matter to invoke the court's jurisdiction." *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). But on a factual attack, a defendant presents extrinsic evidence, so "the court need not presume the truthfulness of the plaintiff's allegations." *Safe Air for Everyone*, 373 F.3d at 1039. "When the defendant raises a factual attack, the plaintiff must support [his] jurisdictional allegations with competent proof, under the same evidentiary standard that governs in the summary judgment context." *Leite*, 749 F.3d at 1121 (citations omitted).

Defendant argues Plaintiffs lack standing to bring their claims because they fail to allege concrete and particularized harm sufficient to establish injury-in-fact. "Article III of the Constitution limits the jurisdiction of federal courts to 'Cases' and 'Controversies.'" *Murthy v. Missouri*, 603 U.S. 43, 56 (2024). And "[a] proper case or controversy exists only when at least one plaintiff establishes that she has standing to sue." *Id.* at 57 (cleaned up). So, a plaintiff must "show that she has suffered, or will suffer, an injury that is concrete, particularized, and actual or imminent[.]" *Id.*

Defendant argues the information it authorized Google to obtain is not individually identifiable and therefore Plaintiffs suffered no harm from its disclosure. Defendant presents a declaration from its expert Kenneth Oliver, who specializes in IP address analysis training. (Dkt. No. 42-1 ¶ 2.) Mr. Oliver testifies there are two types of IP addresses: public and private. (*Id.* ¶¶ 9-21.)[3] Public IP addresses are "shared with the server of every website visited" and are "a globally unique address assigned to a gateway device." (*Id.* ¶¶ 9, 16.) Defendant only collects and shares public IP addresses with Google. (*Id.* ¶ 38.) Most public IP addresses are dynamic, meaning "they change over time." (*Id.* ¶¶ 13, 20.) Mr. Oliver attests that a public IP address can only identify "(1) the name of the ISP ["Internet Service Provider"] who leased the public IP address and (2) general geographic location of the gateway device to which the public IP address was leased (country, city, region, or zip code)." (*Id.* ¶ 28.) So, likening IP addresses to zip codes,

[3] Private IP addresses are device specific and are "not visible to or accessible from the internet or specific webpages." (*Id.* ¶¶ 17-18.)

Defendant argues there is no injury-in-fact from such disclosure. *See Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co.*, 635 Fed. App'x 351, 354 (9th Cir. 2015) ("California does not recognize any common law or constitutional privacy right causes of action for requesting, sending, transmitting, communicating, distributing, or commercially using ZIP Codes.").

Plaintiffs provide their own expert declaration in response. (Dkt. No. 43-1.) Plaintiffs' expert Mr. Greenfield is both a Chief Forensic Examiner and a professor of Information Technology. (*Id.* ¶¶ 3, 4.) While Mr. Greenfield largely agrees with Mr. Oliver's statements, he adds, "[a]t any given moment, no other system can be assigned the same IP address." (*Id.* ¶ 11.) And, "while public IP addresses alone do not provide a users' [*sic*] name, they may act as unique digital identifiers that can correlate to a specific household, workplace, or even an individual system." (*Id.* ¶ 25.)

"When the jurisdictional and merits issues are inseparable, the court must treat a factual attack on jurisdiction as a motion for summary judgment and construe disputed issues of fact in favor of the nonmoving party." *Bowen v. Energizer Holdings, Inc.*, 118 F.4th 1134, 1139 (9th Cir. 2024). In other words, "when jurisdictional issues are 'intertwined with an element of the merits of the plaintiff's claim,' the court must treat the motion like a motion for summary judgment and 'leave the resolution of material factual disputes to the trier of fact.'" *Id.* at 1143 (quoting *Leite*, 749 F.3d at 1121).

Plaintiffs' CMIA claims require finding the information is individually identifying. *See, e.g.*, Cal. Civ. Code § 56.05(j) (requiring a plaintiff alleging violation of the CMIA to prove the information is "individually identifiable"). And the CIPA and California Constitution claims require Plaintiffs have a privacy interest in the collected information. *See, e.g.*, Cal. Penal Code § 632(a) (proscribing against eavesdropping upon "confidential communication"); *Pioneer Elecs. (USA), Inc. v. Superior Ct.*, 40 Cal. 4th 360, 370 (2007) (holding "the right of privacy protects the individual's reasonable expectation of privacy against a *serious* invasion."). So, whether disclosing IP information, when combined with the filtering data, is a concrete and particularized injury ultimately is a question "intertwined with an element of the merits of plaintiff's claim," and as such, the summary judgment standard applies. *Bowen*, 118 F.4th at 1143.

Applying the summary judgment standard, and in light of the current record, the Court cannot find, as a matter of law, that disclosure of Plaintiffs' IP addresses and other information Plaintiffs input into the site—such as their insurance provider, the type of therapy they sought, and their mental health conditions—is not a concrete and particularized injury sufficient to confer standing. In determining statutory standing under CIPA, courts have held IP address collection for targeted advertisement, creates a concrete injury-in-fact. *Compare Mirmalek v. Los Angeles Times Comms. LLC*, No. 24-cv-01797-CRB, 2024 WL 5102709, at *4 (N.D. Cal. Dec. 12, 2024); *and Shah v. Fandom, Inc.*, No. 24-cv-01062-RFL, --- F. Supp. 3d ---, 2024 WL 4539577, at *5 (N.D. Cal. Oct. 21, 2024); *with* Dkt. Nos. 43-1 ¶¶ 22-23; 36 ¶ 45. For example, in *Shah*, the court held "IP addresses reveal geographical location and other personal information sufficient for third parties to conduct targeted advertising." *Shah*, 2024 WL 4539577, at *5.[4] And as Plaintiffs note, HIPAA designates "Internet Protocol (IP) address numbers" as "identifiers of the individual or of relatives, employers, or household members of the individual" that need to be de-identified. 45 C.F.R. § 164.514(b)(2)(i)(O).

Defendant's cited cases do not persuade otherwise. For example, in *United States v. Kidd*, the court reiterated that "most courts have adopted a categorial approach holding that users have no reasonable expectation of privacy in such IP address information." 394 F. Supp. 3d 357, 362 (S.D.N.Y. 2019) (collecting cases). But the *Kidd* court did not stop there. The court analyzed and extensively discussed how other federal and state courts have reached differing conclusions about how to treat IP address collection, usually in the Fourth Amendment context. *Id.* at 362-65. Ultimately, the court disclaimed the categorical approach, finding instead, "under the unique circumstances [that] case presents and the substantial questions the record leaves unresolved, such a rule may not be justified." *Id.* at 368.

In *Hughes v. Vivint*, the plaintiff alleged "harm to be collection of otherwise anonymous information that is used by TikTok to identify Plaintiff through the 'fingerprinting' process." *Hughes v. Vivint*, No. 24-cv-3081-GW-KSx, 2024 WL 5179916, at *5 (N.D. Cal. July 12, 2024).

[4] The *Fandom* court first found the defendants had waived their statutory standing argument, but still proceeded to rule on the standing issue. *Id.*

Because the plaintiff agreed the collected data was "anonymous," the court concluded the plaintiff failed to show "the necessary elements to establish her standing to bring suit." *Id.* The plaintiff did not allege injury because she "fail[ed] to allege that she has a TikTok account that would allow Defendant's collection of her anonymous information from visiting the Website to be associated with her and identify her." *Id.* Here, by contrast, there remains a genuine dispute as to whether the IP information, in conjunction with other information Defendant collected, is personally identifying. While the *Hughes* court found no standing when there was no dispute that the collected information was anonymized, here, no such fact has been indisputably established or alleged. Additionally, Defendant does not contest it incorporates the Google Analytics code on the page where users input personal information to filter for relevant mental-health professionals, (*see* Dkt. No. 42-5) and Plaintiffs attest they did not use VPNs. (Dkt. Nos. 43-2, 43-3.)

Resolution of the standing issue is "intertwined with an element of the merits of plaintiff's claim" and cannot be resolved under the summary judgment standard, *Bowen*, 118 F.4th at 1143, so the Court DENIES Defendant's motion to dismiss under Federal Rule of Civil Procedure 12(b)(1).

II. Motion to Dismiss for Failure to State a Claim (Rule 12(b)(6))

A. CMIA Claim (First Cause of Action)

Plaintiffs allege Defendant violated California Civil Code §§ 56.06, 56.101, 56.10 and 56.36. (Dkt. No. 36 ¶ 107-120.) Section 56.101 prohibits "provider[s] of health care" from "negligently" creating, maintaining, preserving, storing, abandoning, destroying, or disposing of "medical information." Cal. Civ. Code § 56.101. And providers must handle medical information "in a manner that preserves the confidentiality of the information contained therein." *Id.* Section 56.10 prohibits "provider[s] of health care" from "disclos[ing] medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization." And section 56.36 provides statutory damages of up to $1,000 for violations of the Act. Cal. Civ. Code § 56.36(b)(1).

1. "Provider of Health Care"

A "provider of health care" under the CMIA includes, "[a]ny business that offers a mental

health digital service to a consumer … for the diagnosis and treatment of the individual." Cal. Civ. Code § 56.06(d). A "mental health digital service" is "a mobile-based application or internet website that collects mental health application information from a consumer, markets itself as facilitating mental health services to a consumer, and uses the information to facilitate mental health services to a consumer." Cal. Civ. Code § 56.05(l).

Plaintiffs plausibly allege Defendant is a "mental health digital service" and thus a provider of health care under the CMIA. Defendant's "Sessions by Psychology Today" mobile app is specifically designed to aid the "treatment of the individual" since it helps users make and join appointments with therapists. (Dkt. No. 36 ¶ 22, 54, 111.) And Plaintiff D.G. used the app to meet with a therapist. (*Id.* ¶ 22.) Defendant's service allows users "to contact therapists directly," "send[s] consumers emails with the dates and times of their scheduled appointments and a Psychology Today website link to use to check in for their appointments." (*Id.* ¶ 28.) The website collects application information Plaintiffs input prior to connecting to their therapist in addition to collecting Plaintiffs' IP addresses. (*Id.* ¶ 56, 62, 64.) These allegations support a reasonable inference Defendant uses an internet website that collects mental health information to facilitate mental health services to a consumer. Cal. Civ. Code § 56.05(*l*); § 56.06(d).

Defendant insists it is not a mental health digital service because the app is merely its "version of zoom" and is not "software or hardware" as required by the statute. (Dkt. No. 42 at 23-24.) But drawing all reasonable inferences from the allegations in Plaintiffs' favor, as the Court must, Defendant does not "merely" allow Plaintiffs to communicate with therapists such as any video-conferencing app would; instead, Defendant holds itself out as a service that specifically connects users to therapists. (Dkt. No. 36 ¶ 48.)

So, Plaintiffs plausibly plead Defendant is a "provider of health care" under the CMIA.

2. "Medical Information"

For Defendant to be liable under the CMIA, it must have collected "Medical Information" as defined by the statute. Medical information means information that is:

(1) "individually identifiable";

(2) "in possession of or derived from a provider of health care";

(3) "regarding a patient's medical history, mental health application information, . . . , mental or physical condition, or treatment."

Cal. Civ. Code § 56.05(j).

a. "individually identifiable"

"Individually identifiable" means the medical information "includes or contains any element of personal identifying information sufficient to allow identification of the individual." *Id.* Such information includes "the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." *Id.*

Plaintiffs allege Defendant collected their insurance provider, IP addresses, and queries Plaintiffs made regarding their mental health problems. (Dkt. No. 36 ¶¶ 56.) Drawing all reasonable inferences in Plaintiffs' favor, the IP addresses, insurers, mental health status, and treatment information Plaintiffs disclosed, "in combination with other publicly available information," can reveal the identity of individuals using the site. Cal. Civ. Code § 56.05(j); *see also supra* at pp. 6-7. So, Plaintiffs plausibly plead the information is individually identifiable.

b. "regarding a patient's medical history, mental health application information, . . . , mental or physical condition, or treatment"

"Mental health application information" is information "related to a consumer's inferred or diagnosed mental health or substance use disorder … collected by a mental health digital service." Cal. Civ. Code § 56.05(k). "This definition does not encompass demographic or numeric information that does not reveal medical history, diagnosis, or care." *Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 435 (2014).

Plaintiffs allege they made specific queries, including the type of therapy they sought, the faith background of their preferred therapist, their particular mental health issues, and their specific symptoms. (Dkt. No. 36 ¶¶ 11-24.) Plaintiffs therefore plausibly allege they disclosed "Medical Information" within the meaning of the CMIA. In *Eisenhower Medical Center*, 226 Cal. App. 4th at 435, for example, a computer with an index including "each person's name, medical record number (MRN), age, date of birth, and last four digits of the person's Social Security

number (SSN)" was stolen from the defendant. *Id.* at 432. In dismissing the plaintiffs' CMIA claims, the court explained, "under the CMIA a prohibited release by a health care provider must include more than individually identifiable information but must also include information relating to medical history, mental or physical condition, or treatment of the individual." *Id.* at 437. The "mere fact" MRNs were disclosed told little to nothing about what treatment the plaintiffs sought or received. *Id.* at 436. Here, Plaintiffs allege Defendant collected information about which therapists they connected with, the health issues they sought treatment for, and even the type of therapy they sought. These allegations "reveal medical history, diagnosis, or care" as the statute requires. *Id.* at 435.

c. **"in possession of or derived from"**

Finally, Defendant's insistence the medical information was never in its "possession" "or derived from" Defendant and that the information itself did not necessarily relate to Plaintiffs' medical information is unpersuasive. Cal. Civ. Code § 56.05. Drawing all reasonable inferences in Plaintiffs' favor, Defendant's site requested this information from Plaintiffs and Defendant pays Google Analytics to copy this information while it is simultaneously being provided to Defendant; so, Defendant possessed the information and as to Google, it was "derived from" Defendant. Further, Plaintiffs allege the information they input into the site was *their* information. Even if other putative class members potentially did not seek information for their own care, that Plaintiffs here allege they did so is sufficient to survive a motion to dismiss.

***

Accordingly, Plaintiffs plausibly plead the collected information is "medical information" under section 56.05(j).

3. Unauthorized Disclosure under Section 56.10

Under section 56.10(d), health care providers cannot "intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient." Cal. Civ. Code § 56.10(d). And providers cannot "disclose medical information regarding a patient of the provider of health care … to a person or entity that is not engaged in providing direct health care services to the patient." Cal. Civ. Code § 56.10(e). So, a

plaintiff must "plead an 'affirmative communicative act' by the defendant." *Stasi v. Inmediata Health Group Corp.*, 501 F. Supp. 3d 898, 922 (S.D. Cal. 2020) (quoting *Sutter Heath v. Superior Court*, 227 Cal. App. 4th 1546, 1556 (2014)). Disclosure under section 56.10 means "giving out medical information on a patient" and is narrower than the Act's other provisions that merely require "negligently allowing information to end up in the possession of an unauthorized person." *Sutter Health*, 227 Cal. App. 4th at 1554-555 (comparing section 56.10 which proscribes against "disclosure" with section 56.36 which prohibits "negligent release").

Plaintiffs plausibly allege Defendant committed an affirmative communicative act when it shared information to Google by embedding Google Analytics code on its website without anonymization. (Dkt. No. 36 ¶ 117-119.) This code permitted real time sharing with Google of communications inputted by users. (*Id.*) Google then used this information to improve its own business activities and provide "marketing services and offerings," including to other third parties. (*Id.* ¶ 118.)

Defendant laches onto Plaintiffs' allegations of real-time communication and claims a party cannot at the same time affirmatively communicate information and allow a third party to intercept it in real time, (Dkt. No. 42 at 24-25), but this argument mischaracterizes an "affirmative communication." Drawing inferences in Plaintiffs' favor, Defendant "[gave] out medical information" by taking affirmative steps to embed code in its website that did just that. *Sutter Health*, 227 Cal. App. 4th at 1554. Plaintiffs plausibly plead unauthorized disclosure.

4. Unlawful Viewing under Section 56.101

"[I]n order to plead a violation of sections 56.101(a) and 56.36(b), the plaintiff does *not* need to plead an affirmative communicative act." *Stasi v. Inmediata Health Group Corp.*, 501 F. Supp. 3d 898, 922 (S.D. Cal. 2020) (citing *Regents of University of California v. Superior Court*, 220 Cal. App. 4th 549, 553-54 (2013)). The Act *does* require "that negligence resulted in unauthorized or wrongful access to the information,' i.e. that the information was 'improperly viewed or otherwise accessed." *Id.* (citing *Regents*, 220 Cal. App. 4th at 554). Therefore, "a breach of confidentiality under the CMIA requires a showing that an unauthorized party viewed the confidential information." *Vigil v. Muir Med. Grp. IPA, Inc.*, 84 Cal. App. 5th 197, 213

(2022). Unauthorized viewing is critical to a claim under section 56.101. Even when a third party "downloads or copies electronic files" there is no breach of confidentiality under section 56.101 "if the party has not actually viewed the confidential information included in the file." *Id.* at 217.

Google collected the relevant information and used it "for its own purposes including improving and creating new marketing and analytics services for itself." (Dkt. No. 36 ¶ 118.) Google "uses the data to generate reports to help analyze the data collected. This includes reports on acquisition …, engagement …, and demographics." (*Id.* ¶ 44.) Viewing these allegations in the light most favorable to Plaintiffs, a reasonable inference is that Google "viewed or otherwise accessed" this information in order to use it. *Stasi*, 501 F. Supp. 3d at 922 (citing *Regents*, 220 Cal. App. 4th at 554). Plaintiffs have sufficiently alleged unlawful viewing.

***

Because Plaintiffs plead sufficient facts to plausibly support their CMIA claim, the Court DENIES Defendant's motion to dismiss the First Cause of Action.

B. CCPA Claim (Second Cause of Action)

Plaintiffs concede dismissal of this claim. (Dkt. No. 43 at 8 n.1.) Plaintiffs' claim under California Civil Code § 1798.150 is therefore DISMISSED without leave to amend.

C. CIPA § 631 Claim for Aiding and Abetting (Third Cause of Action)

California Penal Code section 631 "prescribes criminal penalties for three distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978).[5] Additionally, section 631 imposes liability "on anyone who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above." *Swarts v. HomeDepot, Inc.*, 689 F. Supp. 3d 732, 743 (N.D. Cal. 2023) (quoting Cal. Penal Code § 631). To adequately plead a civil aiding-and-abetting cause of action under section 631, a party must plead "an underlying predicate violation" by the aided party from one or more of three distinct predicate violations. *B.K. Desert Care Network*, No. 23-cv-05021-SPG (PDx), 2024 WL 1343305, at *7 (N.D. Cal. Feb. 1, 2024). These predicate violations

[5] California Penal Code section 637.2 provides a tort cause of action for violations of sections 631 and 632. *See* Cal. Penal Code § 637.2.

are:

> (1) when a person "by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection … with any telegraph or telephone wire, line, cable, or instrument,"
>
> (2) when a person "willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit," or
>
> (3) when a person "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained."

Yockey v. Salesforce, 688 F. Supp. 3d 962, 970 (N.D. Cal. 2023) (quoting Cal. Penal Code § 631).

As Plaintiffs concede, the first clause "does not apply to the internet, and so cannot support [Plaintiffs'] claims." *Cody v. Ring LLC*, 718 F. Supp. 3d 993, 999 (N.D. Cal. 2024); (Dkt. No. 43 at 26.).

To allege a predicate act under the second clause, a plaintiff must allege the eavesdropping occurred "while the [communication] is in transit." Cal. Penal Code § 631(a). "'While' is the key word here." *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 758 (N.D. Cal. 2023). Plaintiffs allege Google receives information as it is being transmitted, and views and stores the information "to generate reports and to help analyze the data collected." (Dkt. No. 16 ¶¶ 36-39.) The SAC contains detailed allegations of how the software functions and collects information as the user inputs it, and transmits this same information to Google. (Dkt. No. 36 ¶¶ 42-43, 60-61.) However, Plaintiffs do not plausibly allege Google views or reads the information while it is in transit; instead, they allege information is sent "to Google for processing" and later, "[o]nce Google Analytics receives, views, reads, and processes the data, it aggregates and organizes the data based on particular criteria." (*Id.* ¶ 43.) These allegations do not support a plausible inference Google reads the information "while the same is in transit." *See Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096, 1110 (C.D. Cal. 2023) (dismissing section 631 claim when "[t]he timeline of the automatic recording and transcription is unclear."). As such, Plaintiffs fail to adequately allege the second clause predicate act.

Plaintiffs' failure to plausibly allege a violation of the first two clauses defeats any

allegations as to the third. *Tavernetti*, 22 Cal. 3d at 192 (holding the third clause proscribes "attempting to use or communicate information obtained as a result of engaging in either of the previous two activities."); *see also Swarts*, 689 F. Supp. 3d at 744 (holding "[a] violation under the third clause of § 631(a) is contingent upon a finding of a violation of the first or second clause of § 631(a)."); *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 827 (N.D. Cal. 2020) (dismissing aiding-and-abetting claim under the third clause because "Plaintiffs must establish that the information at issue—here, the recordings and transcripts that Defendants' allegedly analyzed—was obtained through a violation of the first or second clauses.")

So, the Court GRANTS Defendant's Motion to Dismiss the Third Cause of Action with leave to amend.

D. CIPA §632 Claim (Aiding and Abetting Liability) (Fourth Cause of Action)

California Penal Code section 632 makes liable "[a] person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication." Cal. Penal Code § 632(a). The section applies to any communications made "by means of a telegraph, telephone, or other device, except a radio." *Id.*

Defendant argues section 632 does not apply to communications made over the internet. The Court disagrees. The statute's plain language reaches communications made through technology or means not enumerated since the statute includes communications made "by means of … [an] *other device*." *Id.* (emphasis added). The only form of communication explicitly excluded by the statute is "radio." *Id.*; *see Green v. California*, 42 Cal. 4th 254, 260 (2007) ("[t]he statute's plain meaning controls the court's interpretation unless its words are ambiguous"); *see also Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1074 (N.D. Cal. 2021) (denying dismissal of section 632 claim when the underlying communications were internet chat messages).

Defendant's reliance on *Swarts* is unavailing. While *Swarts* held "[a] plain reading of the text itself makes clear that the statute only applies to communications transmitted by telephone, not internet," *Swarts*, 689 F. Supp. 3d at 747, the court quotes language from section 632.5, not section 632, to support its holding. *Id.* at 746-47. The distinction is key: section 632 reaches

communications made "by means of a telegraph, telephone, *or other device*," while section 632.5 applies only to communications "between *cellular radio telephones or between any cellular radio telephone and a landline telephone*." *Compare* Cal. Penal Code § 632 (emphasis added); *with* Cal. Penal Code § 632.5 (emphasis added). Thus, while section 632.5's plain text may exclude communications made over the internet, the same is not true for section 632. Defendant fails to persuade section 632 excludes communications sent over the internet.

Defendant also alleges it is not directly liable under § 632 because "a party cannot 'eavesdrop' on their own conversation under the first prong of section 632," and instead Plaintiffs' claim must be analyzed as an aiding-and-abetting claim. *Turner v. Nuance Comms., Inc.*, No. 22-cv-05827-DMR, 2024 WL 2750017, at *8 (N.D. Cal. May 28, 2024). Plaintiffs seemingly agree, arguing in their opposition that its allegations "fully satisfy the common law definition for civil aider-and-abettor liability." (Dkt. No. 43 at 30-31.)

Next, Defendant insists the communications were not "confidential." A confidential communication is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desired it to be confined to the parties thereto." Cal. Penal Code § 632(c). A communication is confidential "if a party has an objectively reasonably expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). A plaintiff "need[] only show a reasonable expectation that the conversation was not being simultaneously disseminated to an unannounced second observer." *Brown*, 525 F. Supp. 3d at 1073 (quoting *Mirkarimi v. Nevada Prop. 1 LLC*, 12-cv-2160-BTM-DHB, 2013 WL 3761530, at *2 (S.D. Cal. July 15, 2013)). California "courts have developed a presumption that Internet communications do not reasonably give rise to that expectation" of privacy. *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (collecting cases). Drawing all reasonable inferences in Plaintiffs' favor, the communications at issue here were confidential. Plaintiffs' communications included personally identifying information, such as their IP addresses, zip codes where they sought medical help, the specific forms of therapy sought (*i.e.*, EFT, CBT), that they sought therapists of a particular faith, and even their insurer.

Defendant's reliance on *Revitch* for the proposition that "[i]nternet communications do not reasonably give rise" to an expectation of privacy is unpersuasive. *Revitch*, 2019 WL 5485330, at *3. In *Revitch*, the court held communications "inquiring about items of clothing on a retail website" were non-confidential as a matter of law. *Id.* But the recorded information here included Plaintiffs' approximate locations, their reasons for seeking therapy, the type of therapy they sought, and their insurers. Indeed, "in recent years, courts in this district have started to recognize that individuals may have a reasonable expectation of privacy for certain internet communications" such as in incognito browsing, personal medical information, and health-related communications. *M.G. v. Therapymatch, Inc.*, No. 23-cv-04422-AMO, 2024 WL 4219992, at *5 (N.D. Cal. Sept. 16, 2024) (collecting cases). So, even accepting that California courts "have developed a presumption that [i]nternet communications do not reasonably give rise to that expectation," *Revitch*, 2019 WL 5485330, at *3 (collecting cases), Plaintiffs sufficiently "plead unique, definite circumstances rebutting California's presumption." *Rodriguez v. Google LLC*, 20-cv-04688-RS, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021).

Finally, Defendant argues Plaintiffs need to allege both it and Google acted "willfully" or "intentionally" to be liable under Penal Code § 632. (Dkt. No. 42 at 28-29, 29-31.) But this standard applies to criminal liability, not civil. Civil aider-and-abettor liability requires "the person (a) knows the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other to so act or (b) gives substantial assistance to the other in accomplishing a tortious result and the person's own conduct, separately considered, constitutes a breach of duty to the third person." *Fiol v. Doellstedt*, 50 Cal. App. 4th 1318, 1325-26 (1996) (quoting *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 846 (1994)). As shown above, Plaintiffs make sufficient allegations to plausibly support an inference that Defendant, at the very least, gave "substantial assistance" to Google, and that Defendant "breach[ed] [its] duty to the [Plaintiffs]" when it shared Plaintiffs' IP addresses and medical information. *Id.*

Defendant's motion to dismiss the Fourth Cause of Action under section 632 is DENIED.

E. California Constitution Claim (Fifth Cause of Action)

To establish a violation of the constitutional right of privacy, plaintiffs "must establish (1)

a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) a serious invasion of the privacy interest." *Int'l Fed'n Pro. & Tech. Eng'rs, Loc. 21, AFL-CIO v. Superior Ct.*, 42 Cal. 4th 319, 338 (2007). Courts consider whether "the intrusion [is] 'so serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *Davis v. Facebook Inc.*, (*In re Facebook, Inc. Internet Tracking Litig.*), 956 F.3d 589, 601 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). Because this inquiry is fact intensive, "[c]ourts are generally hesitant to decide claims of this nature at the pleading stage." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022); *see also Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018) (holding that determinations of whether conduct is highly offensive "is indeed a factual question best left for a jury.").

First, as noted *supra*, at pp. 6-7, Plaintiffs sufficiently plead a privacy interest and a reasonable expectation of privacy in the information Google Analytics collected through Defendant's site. Further, Plaintiffs plead sufficient facts to "constitute an egregious breach of the social norms." *In re Facebook, Inc. Internet Tracking Litig.*, 956, F.3d at 601. In determining offensiveness, courts consider "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994). Plaintiffs allege Defendant shared information they communicated to it while seeking treatment for their mental health conditions. (Dkt. No. 16 ¶ 155.) This intrusion upon their privacy included the dissemination of personally identifying information. Drawing all reasonable inferences in Plaintiffs' favor, the Court cannot conclude as a matter of law such conduct was not highly offensive. When Plaintiffs "allege[] Defendant implemented a system that surreptitiously allowed third parties, …, to track, record, and intercept [their] and other online patients' confidential communications, personally identifiable information, and [Personal Health Information], and use that information for marketing and other purposes … that is sufficient to allege that Defendant's conduct was highly offensive." *St. Aubin v. Carbon Health Techs., Inc.*, No. 24-00667-JST, 2024 WL 4369675, at *13 (N.D. Cal. Oct. 1, 2024).

Defendant's motion to dismiss Plaintiffs' Sixth Cause of Action is DENIED.

CONCLUSION

The Court rules as follows:

- Defendant's motion to dismiss for lack of subject matter jurisdiction under Federal Rule of Federal Procedure 12(b)(1) is DENIED because material issues of fact intertwined with the merits exist regarding injury-in-fact.
- Defendant's motion to dismiss Plaintiffs' First Cause of Action under the CMIA is DENIED.
- Defendant's motion to dismiss Plaintiffs' Second Cause of Action under the CCPA is GRANTED without leave to amend.
- Defendant's motion to dismiss Plaintiffs' Third Cause of Action under California Penal Code § 631 is GRANTED with leave to amend.
- Defendant's motion to dismiss Plaintiffs' Fourth Cause of Action under California Penal Code § 632 is DENIED.
- Defendant's motion to dismiss Plaintiffs' Fifth Cause of Action under the California Constitution is DENIED.

Any amended complaint is to be filed no later than April 24, 2025. The Court shall hold a case management conference via Zoom video on May 26, 2026 at 2:00 p.m. A joint case management conference statement is due one week in advance.

This Order disposes of Docket Number 42.

IT IS SO ORDERED.

Dated: March 28, 2025

JACQUELINE SCOTT CORLEY
United States District Judge

United States District Court
Northern District of California